Security Architecture and Design Documentation Guidance

HIGH LEVEL DESIGN (HLD)

Version 1.4

Prepared by HR CDS TT

23 June 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HR CDS TT	24 May 2010	Document creation	1.0
HR CDS TT	11 June 2010	Edits and additions	1.1
HR CDS TT	16 September 2010	Edits and additions	1.2
HR CDS TT	3 March 2011	Review and update by Tiger Team	1.3
HR CDS TT	23 June 2011	Update by Tiger Team	1.4

ACRONYMS AND DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Development Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SFS	Security Functional Specification
SP	Security Policy

INTRODUCTION

The high level security design of a system provides a description of the security functions in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high level design provides evidence that the system architecture is appropriate to implement the system's security functional requirements.

The high level design refines the Security Functional Specification (SFS) into subsystems. For each subsystem, the high level design describes its purpose and function, identifies the security functions contained in the subsystem, and describes interrelationships among subsystems. These interrelationships will be represented as interfaces for data flow, control flow, etc., as appropriate. The same information will be provided for external system interfaces.

The design description of a system provides both context for a description of the security functions, and a thorough description of the system's security functions. As assurance needs increase, the level of formalism/rigor provided in the description also increases. As the size and complexity of the systems security functions increase, several levels of decomposition may be appropriate. The design description is intended to provide information, commensurate with the given assurance level, so that a determination can be made that the security functional requirements are realized.[1]

Figure 1 shows the relationship of the HLD to the other topic areas described in the DRD.

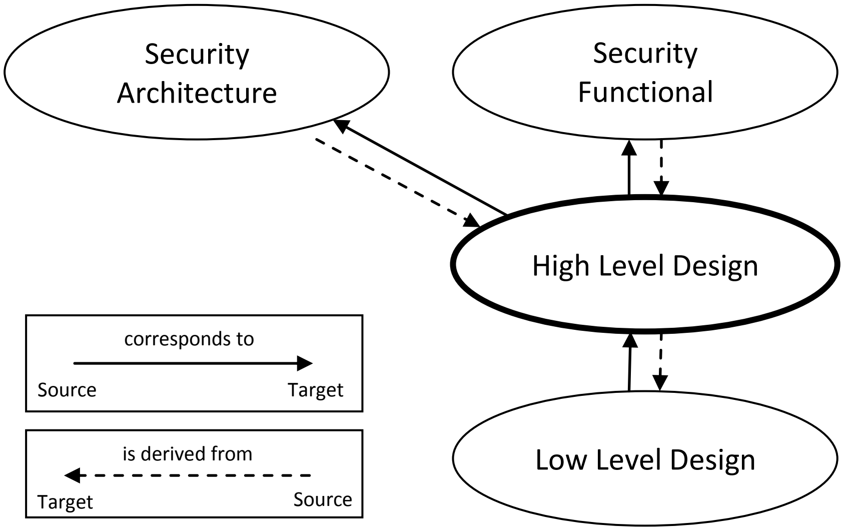

Figure 1 – High Level Deisgn Interactions

[1] The HLD applies to the solution to be evaluated, which may only be an application that is based on an evaluated foundation or it must address both the application and the foundation.

DISCUSSION

Design documentation typically describes two levels of decomposition: subsystem and module. A subsystem provides a high level description of what a portion of the system is doing and how. As such, a subsystem may be further divided into lower-level subsystems, or into modules. A module is the most specific design description of functionality: it is a description of the implementation.

The high level design (HLD) will typically describe one or two levels of subsystems in order to adequately convey a useful description of how the system works. The low level design (LLD) further expands the subsystem description to the module level.

The term “security functionality” represents the set of security operations that a system provides. A subsystem may provide complete security functions or may contribute to one or more security functions. This distinction is made because design constructs, such as subsystems and modules, do not necessarily relate to specific security functions. While a given subsystem may correspond directly to a security function, or even multiple security functions, it is also possible that many subsystems must be combined to implement a single security function.

The goal of the HLD is to define the system security boundary and to describe for each subsystem:

- the security enforcing functionality,
- the security supporting functionality, and
- the security non-interfering functionality.

The HLD describes an accurate and complete instantiation of the system’s security architecture and security functions.

REQUIREMENTS

HLD-1 The developer shall provide the high level design of the system.

HLD-2 The HLD shall describe the system architecture in terms of subsystems.

HLD-3 The HLD shall include a system level, architectural diagram that graphically depicts the subsystems, their interrelationships and the flows among them.

HLD-4 The HLD shall be written in [selection: informal, semiformal] language, as specified in the DRD.

HLD-5 The HLD shall describe a high level design of the security functions

HLD-6 The HLD shall include diagrams that highlight the security relevant information controls and flows.

HLD-7 The HLD shall identify all subsystems within the system security boundary, indicating whether they are security enforcing, supporting and/or non-interfering.

HLD-8 The HLD shall, for each security function, identify the implementing subsystems.

HLD-9 The HLD shall describe the role each subsystem plays in implementing the security function.

HLD-10 The HLD shall, for all subsystems in the security boundary, identify all interfaces and their purpose.

HLD-11 The HLD shall, for each security enforcing and security supporting subsystem, identify the assumptions on inputs and assertions on outputs for the subsystem's external interfaces.

HLD-12 The HLD shall, for each subsystem, describe its behavior in sufficient detail to validate its role as security enforcing, security supporting, and/or security non-interfering.

HLD-13 The HLD shall describe any assumptions made regarding the security behavior of the foundation.

HLD-14 The HLD shall describe the extent to which the foundation has been evaluated.

HLD-15 The HLD shall describe any environmental assumptions regarding external functionality that may affect the security of the system.

HLD-16 The HLD shall, for each security enforcing subsystem, describe its interactions with other subsystems.

HLD-17 The HLD shall describe how the security enforcing subsystems are protected from all other subsystems.

HLD-18 The HLD shall describe the system philosophy of protection2 showing how the security mechanisms satisfy the security requirements.

HLD-19 The HLD shall be internally consistent (the statements and diagrams do not contradict themselves and each other).

[2] Fill in reference